REMARKS

We have amended claims 1 and 47. Claims 1, 2, 4-20, 31, and 38-48 are pending in the application.

The examiner rejected claims 1-4, 9-11, 14-17, 31, 33, 37-41, 43, and 47 under 35 U.S.C. §103(a) as being unpatentable over Jones (5,623,637) in combination with Shamir. The examiner argues that Jones discloses everything in the claims except for "a protocol wherein the client has a client secret and the server has a server secret used to compute a third secret from the client and server secret and the server cannot feasibly determine the client secret or the third secret." The examiner argues that Shamir teaches that which is missing from Jones. We disagree. Shamir actually teaches less than the examiner believes. Specifically, among other things, Shamir does not teach a method "wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret or the third secret," as is recited in claim 1 as amended.

The secret sharing scheme disclosed by Shamir is intended to prevent a number of entities from knowing a secret by distributing parts of the secret among those entities. The scheme requires some number of the entities to cooperate in order to obtain the secret, and thus prevents any one entity from obtaining and misusing the secret. For example, Shamir describes that if "each executive is given a copy of the company's secret signature key, the system is convenient but easy to misuse" (p. 612). In other words, an entity that knows the secret could misuse it without the cooperation or knowledge of others.

To this end, Shamir teaches a method where, for example, "each executive is given a small magnetic card with one D_i piece." The pieces can then be used together at a "signature generating device...in order to generate (and later destroy) a temporary copy of the actual signature key D." But the secret is not revealed to any of the executives, because then they could "misuse" it. This violates the requirement of claim 1, which recites that "the client obtains the third secret." According to the scheme of Shamir, none of the entities possessing secret parts (e.g., the client or server) can obtain the secret (e.g., the third secret).

Claim 38 recites "at the client deriving a password from the third secret," and thus distinguishes Shamir for the reasons described above. Shamir teaches a system in which an entity possessing a secret part cannot obtain the secret (e.g., the third secret) and thus would not be able to derive a password from that secret, as is recited in the claim.

Claim 47 recites "no additional multi-party secure computation protocol involving any entity other than the server is required to enable the client to generate the third secret and the key derived from the third secret." In contrast, Shamir teaches a system in which an entity possessing a secret part cannot obtain the secret (e.g., the third secret) and thus would not be enabled to either generate that secret or a key derived from that secret, as is recited in the claim.

Therefore, the claims are patentable over Jones in combination with Shamir. None of the other art cited by the examiner supplies that which is missing from Jones and Shamir.

For at least the reasons stated above, applicants believe the pending application is in condition for allowance.

Applicants hereby request a three-month extension of time to extend the period of response. Please charge the extension fee for this request to Deposit Account No. 08-0219.

Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Dated: November 7, 2005

Respectfully submitted,

By _____

Eric L. Prahl
Registration No.: 32,590
WILMER CUTLER PICKERING HALE AND DORR LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000
Attorney for Applicant